Efisiensi Biaya Audit melalui Peningkatan Pengendalian Umum dan Aplikasi pada Bisnis Factory Outlet (Kasus pada Siklus Penjualan F O O01 di Bandung)

Elizabeth Tiur Manurung
Program Studi Akuntansi, Fakultas Ekonomi,
Universitas Katolik Parahyangan, eliz@unpar.ac.id

Chintia Tanjung Kumala
Program Studi Akuntansi, Fakultas Ekonomi,
Universitas Katolik Parahyangan, chintiatanjungkumala@yahoo.com

Abstract

The purpose of this study is to know the result of evaluation of the general control and application control of sales cycle in relation with audit scope and audit expense. By used the Analytical descriptive research method, and the research object is one of factory outlet in Bandung, research resulted in the conclusion that general control and application control of sales cycle was satisfy.

The company has applied all components that will increase control in sales cycle by using Corsus software 1.1.62, such as keeping up IT administration, developing system, secure control for hardware and online. In input control, scanning of product barcode by cashier will be compared with inventory code in Corsus, and securing the validity of input data will increase the input control, while Corsus also has implemented log fiture that recorded all cashier activites in point of sales module. As the company has a very satisfied IT control then this will reach up in the lower risk control. This fact will influence the scope of audit in many aspect like nature, timing, extent and staffing. Furthermore, all this aspect will come up to decrease the audit expenses.

Abstrak

Penelitian ini bertujuan untuk mengetahui hasil evaluasi pengendalian umum, dan pengendalian aplikasi pada siklus penjualan dihubungkan dengan luas audit dan biaya audit. Dengan menggunakan metode deskriptif analitis, dan objek penelitian salah satu Factory Outlet di Bandung, hasil penelitian menunjukkan bahwa pengendalian umum dan aplikasi siklus penjualan telah memadai.

Perusahaan menggunakan *Software Corsus* 1.1.62 untuk menerapkan semua komponen pengendalian, seperti adanya administrasi IT, pengembangan sistem, pengamanan fisik *hardware* dan *on line*. Pada input control, *scanning barcode*

Jurnal Administrasi Bisnis (2014), Vol.10, No.1: hal. 1–16, (ISSN:0216–1249)

produk yang dilakukan kasir akan dicocokkan oleh Corsus dengan kode persediaan, adanya pengendalian validitas input, serta adanya modul implementasi fitur log yang mencatat semua aktivitas kasir selama melakukan penjualan, telah turut meningkatkan pengendalian aplikasi siklus penjualan. Pengendalian yang memadai atas implementasi ini, mengakibatkan turunnya risiko aktivitas penjualan sehingga akan mengurangi luasnya audit dari sudut sifat, waktu, kedalaman, serta staf yang digunakan sehingga akan menurunkan biaya audit.

Keywords: IT control, general control, application control, audit scope, audit expense

1. Pendahuluan

1.1. *Latar Belakang*

Bisnis Factory Outlet di Bandung terus tumbuh sesuai meningkatnya permintaan masyarakat, bukan hanya dari penduduk Bandung tetapi juga dari luar Kota Bandung terutama Jakarta, bahkan dari Luar Negeri misalnya Malaysia, Singapore, Belanda, Australia (Pikiran Rakyat; 1 Feb 14, h.22).

Suatu perusahaan didirikan untuk tujuan memperoleh keuntungan yang optimum, demikianpun dengan sebuah Factory Outlet. Pemilik ingin mengukur apakah kinerja perusahaan baik atau tidak. Salah satu cara mengukur kinerja bisnis adalah melalui laporan keuangan yang disusun oleh perusahaan. Agar laporan keuangan terbebas dari praduga mengandung kesalahan, maka perlu diaudit oleh pihak yang independen misalnya Akuntan Publik. Audit atas suatu laporan keuangan membutuhkan biaya yang tidak sedikit.

Langkah awal mengaudit suatu laporan keuangan adalah dengan mengevaluasi pengendalian intern yang terdapat dalam perusahaan. Bila perusahaan menyelenggarakan pengendalian yang baik, maka laporan keuangan yang dihasilkan berisiko kecil menghasilkan kesalahan, sebaliknya pengendalian yang lemah akan menghasilkan laporan yang memiliki risiko besar mengandung kesalahan.

Dewasa ini, banyak perusahaan menggunakan teknologi informasi (IT) dalam menjalankan pengendalian operasi perusahaannya. Menggunakan teknologi, akan dihasilkan pemrosesan data yang lebih efisien dengan waktu lebih singkat. Arens, et.al (2012, h.390-391) mengelompokkan IT control ke dalam *General control* (Pengendalian umum) dan *Application control* (pengendalian aplikasi). Informasi yang dihasilkan lebih berkualitas, karena diproses secara konstan sehingga salah saji akan berkurang serta mengurangi risiko laporan keuangan mengandung kekeliruan, sehingga biaya atas audit yang dilakukan dapat diperkecil.

1.2. *Rumusan Masalah*

Berdasarkan latar belakang masalah yang telah diungkapkan di atas, maka perumusan masalah yang diteliti, adalah sebagai berikut.

i Bagaimana hasil pemeriksaan atas Pengendalian umum sistem teknologi informasi secara keseluruhan dan Pengendalian aplikasi pada siklus penjualan pada perusahaan O01?

ii Bagaimana menentukan ruang lingkup audit berdasarkan hasil pemeriksaan Pengendalian umum dan aplikasi tersebut?

iii Apakah Pengendalian umum dan aplikasi yang diterapkan perusahaan dapat mengurangi biaya audit?

1.3. *Kerangka Pemikiran*

Gambar (1) menggambarkan tentang skema kerangka pemikiran. Peningkatan penggunaan teknologi pada sistem informasi akuntansi, bermanfaat dalam memproses data dengan konsisten, dengan volume yang besar, serta mengurangi risiko akibat *human error*. Walaupun teknologi informasi juga tetap berisiko, misalnya risiko terkait *hardware* dan data, kurangnya *audit trail*, kebutuhan akan ahli di bidang IT dan pemisahan fungsi IT.

Perusahaan perlu menambahkan *IT controls* dalam pengendalian internnya sebagai respon atas risiko di atas. *IT controls* terdiri dari pengendalian umum yang bersifat *pervasive*, berlaku untuk semua aspek pemrosesan data dengan IT. Sedangkan pengendalian aplikasi berlaku untuk pemrosesan transaksi dan hanya terkait dengan program yang digunakan. Pengendalian umum memberikan kewajaran yang memadai bahwa pengendalian aplikasi telah berjalan secara efektif (Arens, et.al, 2012, h.374).

Auditor mesti memahami pengendalian umum dan pengendalian aplikasi yang dilakukan klien, melalui observasi, wawancara dengan karyawan yang menggunakan IT dan penyebaran kuesioner untuk mengidentifikasi pengendalian intern secara spesifik. Jika hasil pengujian dinilai sudah efektif, maka auditor dapat mengurangi *scope* auditnya, dengan kata lain biaya yang diperlukan atas audit akan berkurang (Arens, et.al, 2012: 374).

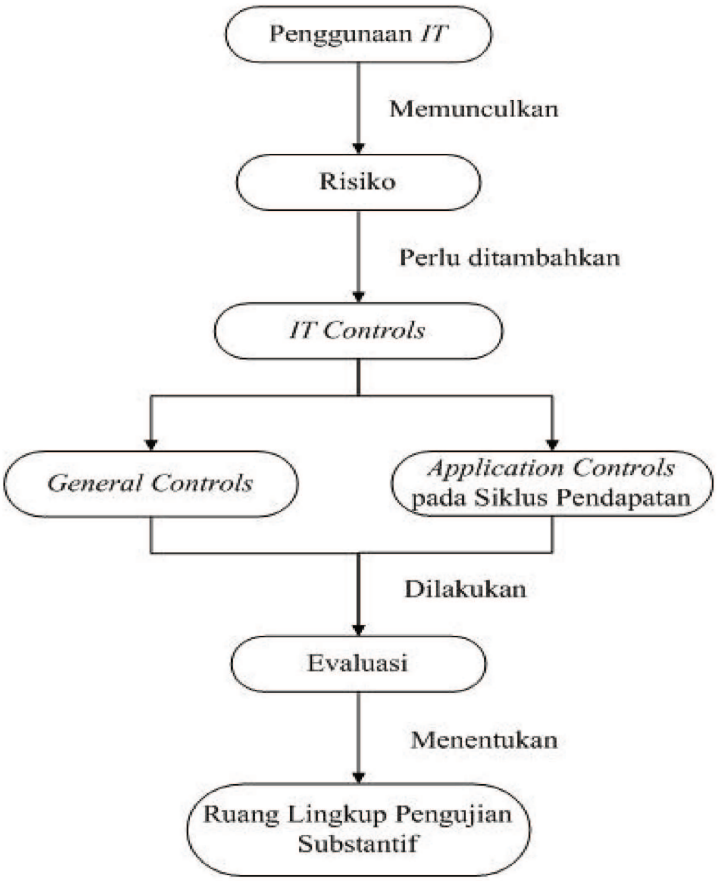
2. Studi Literatur

2.1. *Audit*

Audit merupakan proses mengumpulkan dan mengevaluasi bukti, menentukan tingkat kesesuaian atas asersi manajemen dengan kriteria yang berterima umum. Seorang auditor harus kompeten dan independen (Arens et.al, 2012, h.24).

2.2. *Asersi Manajemen*

Arens et.al (2012, h.173) menyatakan asersi manajemen sebagai ungkapan manajemen tentang transaksi yang terjadi disertai pengungkapan yang terdapat dalam



Gambar 1. Skema Kerangka Pemikiran (Arens, et.al., 2012, h374)

laporan keuangan. Audit berkaitan erat dengan asersi manajemen. Audit merupakan proses membandingkan antara informasi (laporan keuangan) dengan kriteria (standar) yang telah ditentukan. Oleh karena itu, auditor harus memahami asersi manajemen dalam melakukan audit.

Asersi dibagi menjadi tiga kategori sesuai dengan ISA (IAASB, 2012, h.301-302), yaitu

1. Asersi terkait kelas transaksi, terdiri dari: *occurrence, completeness, accuracy, classification, cut off*. *Occurance* berarti semua transaksi yang dicatat memang terjadi. *Completeness* berarti semua transaksi yang seharusnya dicatat telah dicatat. *Accuracy* berarti jumlah atau nominal transaksi telah dicatat dengan sesuai. *Classification* berarti transaksi telah dicatat pada akun yang sesuai. *Cut off* berarti transaksi telah dicatat pada periode akuntansi yang benar;

2. Asersi terkait saldo akun pada akhir tahun, terdiri dari: keberadaan transaksi, kelengkapan, penilaian dan klasifikasi, hak & kewajiban;

3. Asersi terkait penyajian dan pengungkapan, terdiri dari: keterjadian transaksi dan hak serta kewajiban, kelengkapan, ketepatan dan penilaian, pengklasifikasian dan *understandability*.

2.3. *Audit Risk Model*

Statement on Auditing Standards AU 3122.02 (SAS 47) seperti yang dikutip oleh Boynton dan Johnson (2006, h.194) mengartikan *audit risk* sebagai risiko auditor tidak mengetahui kegagalan dalam penentuan opini atas laporan keuangan yang sebenarnya mengandung salah saji material. Auditor menjabarkan *audit risk* sebagai fungsi dari *inherent risk, control risk, dan detection risk* (Boynton dan Johnson, 2006, h.194-196).

Inherent risk adalah kerentanan asersi terhadap salah saji yang material, dengan mengasumsikan tidak ada pengendalian intern terkait. Penilaian inherent risk sangat bergantung pada karakteristik yang unik pada bisnis klien, seperti yang dikutip oleh Hall (2005, h.10). *Control risk* adalah risiko salah saji material pada asersi karena pengendalian intern tidak mampu mendeteksi salah saji tersebut. Control risk dinilai rendah jika pengendalian intern efektif, yaitu mampu mencegah atau melakukan koreksi atas salah saji.

Auditor melakukan penilaian atas *control risk* dengan melakukan *test of controls*. *Detection risk* adalah risiko auditor tidak dapat mendeteksi adanya salah saji material pada sebuah asersi. *Detection risk* yang rendah berarti kemungkinan gagal yang rendah atas pengujian asersi secara langsung oleh auditor untuk mendeteksi salah saji yang material.

2.4. *Ruang Lingkup Audit Penjualan*

Berbagai pengujian dilakukan oleh auditor untuk meyakinkan kewajaran setiap asersi pada laporan keuangan, atau adakah salah saji material pada laporan keuangan. Auditor harus menentukan ruang lingkup audit sebagai dasar dalam menentukan opini atas kewajaran laporan keuangan klien.

Boynton dan Johnson (2006, h.523-531) menjabarkan empat keputusan yang harus diperoleh auditor, yaitu:

a) *Nature of substantive test*, merujuk kepada tipe dan efektivitas pengujian audit yang akan dijalankan;

b) *Timing of substantive test*, adalah keputusan auditor mengenai waktu pengujian substantif dilaksanakan, apakah saat tanggal neraca atau sebelum tanggal neraca;

c) *Extent of substantive test*, merujuk kepada penggunaan sample size dalam pengujian substantif;

d) *Staffing of substantive test*, Keputusan staffing terkait dengan penugasan staf yang berpengalaman, peningkatan pengawasan audit, atau penggunaan spesialis dalam bidang ilmu lain.

2.5. *Pengendalian Intern*

Menurut *COSO Internal Control Framework* seperti yang dikutip oleh Moeller (2007, h.4), pengertian pengendalian intern adalah proses, yang dipengaruhi oleh dewan direksi, manajemen dan anggota lain, dan dirancang untuk memberikan kepastian yang layak mengenai pencapaian tujuan manajemen, yaitu efektivitas dan efisiensi operasi, keandalan pelaporan keuangan, serta ketaatan pada hukum dan peraturan.

2.6. *Komponen Pengendalian Intern*

COSO Internal Control Intergrated Framework, seperti dikutip oleh Arens, et. al (2012, h.314-322) menguraikan lima komponen agar tujuan pengendalian tercapai, antara lain:

1) *Control environment* yang terdiri dari tindakan, kebijakan, prosedur yang mencerminkan sikap manajemen tingkat atas, direktur, dan pemilik mengenai pentingnya pengendalian intern;

2) *Risk assessment* - Penilaian risiko dilakukan manajemen dengan mengidentifikasi dan menganalisis risiko laporan keuangan serta kesusuaiannya dengan standar akuntansi;

3) *Information and communication* - Tujuan sistem informasi akuntansi dan komunikasi untuk menginisiasi, mencatat, memproses, dan melaporkan transaksi entitas dan menjaga akuntabilitas aset;

4) *Monitoring* - berkaitan penilaian secara periodik atas kualitas pengendalian intern untuk menentukan bahwa pengendalian beroperasi seperti yang diharapkan dan telah dimodifikasi sesuai perubahan yang terjadi;

5) *Control activities* - merupakan kebijakan dan prosedur yang digunakan untuk memastikan tindakan yang dibutuhkan telah diambil untuk menangani risiko sehingga tujuan tercapai.

2.7. *Information Technology (IT) Controls*

Komputer berkemampuan untuk memproses informasi secara konsisten sehingga sistem IT dapat mengurangi salah saji secara otomatis dan dengan biaya yang rendah.

Hall (2005, h.24) membagi control activities menjadi dua, yaitu: *computer* dan *physical*. Pengendalian atas *computer* sangat berkaitan dengan IT *environment* dan IT *auditing*. Selaras dengan Arens, Hall juga membagi pengendalian atas computer menjadi *general control* dan *application control*

2.8. *General Control*

General control berlaku untuk semua aspek dalam penggunaan IT. Menurut Arens, et. al (2012, h.394-398) terdapat enam kategori dari general control, yaitu:

1. Administrasi IT bagaimana sikap dewan direksi dan manajemen senior terhadap penggunaan IT dan seberapa penting IT tersebut dalam organisasi. Jika penyelesaian permasalahan IT diserahkan kepada manajemen tingkat bawah atau menggunakan konsultan IT, maka ini menandakan bahwa IT bukan prioritas.

2. Pemisahan fungsi IT. Keterbatasan sumber daya, mengakibatkan perusahaan tidak mampu menerapkan segregation of IT duties. Namun, beberapa fungsi penting tetap mesti dipisahkan, seperti (Rittenberg; 2005, h.208):

   a Operator komputer dengan fungsi programming jika tidak operator dapat mengakses system logs, sehingga dapat membuat perubahan yang tidak diotorisasi dan tidak terdeteksi pada program atau data.

   b *Computer program librarian* dengan fungsi yang lainnya. Akses ke program dan data harus dibatasi, akses hanya diperbolehkan untuk pengguna dengan tujuan yang diotorisasi.

   c *Database administrative* dengan data input function. *Database administrator* harus menjaga integritas dari database, sedangkan user bertanggung jawab atas kelengkapan dan integritas input ke dalam database.

3. Pengembangan sistem. Aktivitas dalam pengembangan sistem termasuk:

   a) Pembelian software atau pengembangan *in-house software;*

   b) Pengujian semua software untuk memastikan bahwa software cocok dengan hardware dan software yang sudah ada dan menentukan apakah hardware dan software dapat menangani jumlah transaksi yang dibutuhkan. Perusahaan menggunakan dua pendekatan pengujian software:

      i *Pilot testing* : sistem diimplementasikan pada satu bagian dan bagian lainnya masih menggunakan sistem yang lama.

      ii *Parallel testing* : sistem yang lama dan baru bekerja secara sekaligus pada semua bagian di organisasi.

4. Pengamanan fisik dan online. Pengendalian fisik dan pembatasan hak akses atas software dan data akan mengurangi risiko atas perubahan yang tidak terotorisasi, dan penggunaan yang tidak seharusnya atas program dan data. Pengendalian fisik yang layak atas peralatan komputer dimulai dengan membatasi akses ke hardware, software, serta backup file data.

   Contohnya kamera keamanan, personil keamanan (satpam), atau izin akses fisik dan akses online setelah sidik jari retina karyawan dicocokan dengan database yang disahkan. Pengendalian akses online meliputi penggunaan user IDs dan password,firewall dan enkripsi.

5. *Backup and Contingency Planning* – untuk mencegah risiko kehilangan data saat putusnya sambungan listrik, digunakan baterai atau generator listrik. Untuk bencana yang lebih serius, harus dibuat backup dan contingency terkait penyimpanan data dan program, di tempat tertentu atau menggunakan jasa perusahaan lain.

6. *Hardware Controls*. *Hardware controls* ditambahkan dalam komputer oleh pabrik pembuatnya untuk mendeteksi dan melaporkan kegagalan peralatan. Auditor memperhatikan tindakan klien saat menangani kesalahan yang diidentifikasi oleh hardware controls.

2.9. *Application control*

Arens, et. al (2012, h.398) berpendapat bahwa *application control* dirancang untuk *software application*, ditujukan untuk membantu dalam memenuhi audit objektif. *Application control* dilakukan oleh komputer, disebut dengan a*utomated controls*, maupun oleh manusia, disebut *manual controls*. *Application control* dibagi menjadi tiga kategori (Arens, et. al, 2012, h.398-400), yaitu:

1. *Input Controls* - untuk memastikan informasi yang dimasukkan ke dalam komputer telah diotorisasi, akurat, dan lengkap. Kesalahan pada *IT systems* sebagian dihasilkan dari kesalahan saat *data entry*. Tipe pengendalian manual dapat digunakan dalam *input controls* adalah:

   a Otorisasi manajemen atas transaksi;

   b Kecukupan dokumen sumber sebagai dasar input data; dan

   c Karyawan yang kompeten.

   Sedangkan menurut Romney dan Steinbart (2009, h.322-323), pengendalian data sumber terdiri dari:

   a *Forms design*. Dokumen sumber dan formulir didesain untuk mengurangi kesalahan dan kelalaian. Terdapat dua pengendalian utama yaitu memberikan nomor urut pada dokumen (prenumbered document) dan menggunakan dokumen turnaround. Urutan nomor pada dokumen dapat mengendalikan serta mendeteksi dokumen yang hilang. Dokumen *turn-around* adalah catatan data perusahaan yang dikirim ke pihak luar dan dikembalikan ke sistem sebagai input.

   b *Cancellation and storage of documents*. Dokumen yang telah dimasukkan ke dalam sistem harus dicap batal agar tidak dimasukkan kembali, baik sengaja maupun tidak.

   c *Authorization and segregration of duties*. Dokumen sumber disiapkan oleh personil yang diotorisasi dan bertindak sesuai dengan otorisasinya.

   d *Visual scanning*. Dokumen sumber dipindai untuk memastikan kelogisan dan kepemilikan sebelum dimasukkan ke dalam sistem.

   Selain itu, menurut Romney dan Steinbart (2009, h.323), terdapat beberapa pengendalian *data entry* untuk memastikan validasi input sebagai berikut:

   a. *Field check* menentukan apakah jenis karakter di dalam field sesuai atau tidak;

b. *Sign check* menentukan apakah data di dalam field memiliki tanda aritmatik yang sesuai;
c. *Limit check* menguji jumlah numerik bahwa jumlah tersebut tidak melebihi nilai yang sudah ditentukan sebelumnya.
d. *Range check* serupa dengan limit check, kecuali dalam hal batas atas dan batas bawah
e. *Size check* memastikan bahwa data akan cocok dengan field-nya
f. *Completeness check* memastikan bahwa semua data yang diperlukan telah dimasukkan
g. *Validity check* membandingkan nomor ID atau kode transaksi dengan yang telah diotorisasi
h. *Reasonableness test* menentukan ketepatan logis dari data yang dimasukkan dan disimpan
i. *Check digit verification* memeriksa check digit, yang merupakan digit lain yang dihitung dari ID atau kode yang telah diotorisasi

2. *Processing Controls*. *Processing controls* untuk mencegah dan mendeteksi kesalahan pada saat pemrosesan transaksi. Romney dan Steinbart (2009: 325) menjabarkan pengendalian untuk mempertahankan integritas pemrosesan data:

a. *Data matching*. Dua atau lebih data harus dicocokkan sebelum tindakan lebih lanjut dilakukan pada kasus tertentu
b. *File labels*. *Label file* harus dicek untuk memastikan file sudah benar sudah diperbaharui
c. *Recalculation of batch totals*. *Batch total* dihitung kembali pada setiap record transaksi yang diproses
d. *Cross-footing and zero balance test*. *Cross-footing balance test* digunakan untuk membandingkan hasil yang ada dengan metode tertentu untuk menilai keakuratan. Sedangkan zero balance test menerapkan logika yang sama untuk pengendalian suatu akun.
e. *Write-protection mechanisms*. Perlindungan terhadap penulisan atau penghapusan arsip data yang tidak sengaja dalam media magnetik
f. *Database processing integrity procedures*. Sistem database menggunakan *database administrator*, *data dictionaries*, dan *concurrent update controls* untuk memastikan integritas proses. *Concurrent update controls* melindungi records dari kesalahan yang terjadi ketika terdapat dua atau lebih user meng-update record yang sama.

3. *Output Controls*. *Output controls* berfokus mendeteksi kesalahan setelah pemrosesan data selesai. Pengendalian penting dalam output controls adalah peninjauan data *reasonableness* oleh orang berpengetahuan luas atas output tersebut. Sedangkan menurut Romney dan Steinbart (2009:326), output controls terdiri dari:

a. *User review of output* para user harus memeriksa kelogisan, kelengkapan, dan kecocokan sistem output yang mereka peroleh

b. *Reconciliation procedures* akun dalam general ledger harus direkonsiliasi secara berkala dengan total akun subsidiary

c. *External data reconciliation* total database harus direkonsiliasi secara berkala dengan data di luar sistem

3. Metode dan Obyek Penelitian

Penelitian ini menggunakan metode deskriptif analitis, yaitu melakukan pengumpulan dan penganalisisan data untuk memperoleh gambaran yang jelas atas objek penelitian, lalu menarik kesimpulan dan memberikan saran.

Variabel penelitian yang digunakan adalah evaluasi general control dan application control atas siklus penjualan pada FO O01, serta ruang lingkup pengujian substantif dan Biaya audit, dengan catatan audit yang dilakukan juga pada siklus audit. Objek penelitian adalah FO O01, merupakan *lifestyle concept store* yang berada di Jalan Setiabudhi Bandung. Istilah *concept store* memiliki perbedaan dengan *department store. Concept store* yaitu sebuah pusat perbelanjaan yang menyediakan berbagai produk mulai dari pakaian, aksesori, perlengkapan rumah, alat tulis, dengan koleksi produk yang lebih unik dan ekslusif serta mengusung tema tertentu. Lantai pertama toko digunakan untuk aksesoris, pakaian anak, pakaian perempuan, dan pakaian laki-laki serta di bagian kiri terdapat taman kecil tempat memajang tanaman yang akan dijual dan peralatan rumah tangga. Lantai kedua tempat untuk pernak pernik dan peralatan rumah tangga.

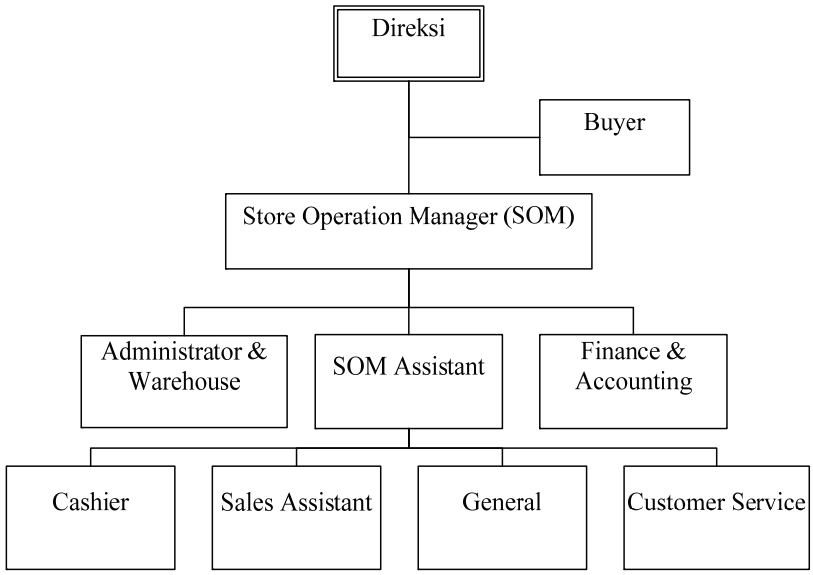
Perusahaan menggunakan software Corsus versi 1.1.62 pada *cash register* yang telah terintegrasi dengan barcode dalam melakukan proses penjualan. Perusahaan tidak menggunakan semua modul yang ada pada software Corsus, hanya modul POS (*Point of Sales*) atau *direct sales*. Beberapa modul yang disediakan oleh Corsus tidak sesuai dengan karakteristik industri retail. Karyawan pada bagian ini yang dapat menggunakan komputer, yaitu Kasir, *Warehouse*, Administrator, *Finance Accounting*, SOM Assistant atau SOM, Direksi.

4. Hasil Penelitian Dan Analisis

4.1. *Hasil Pengujian Pengendalian Umum*

Berikut adalah rangkuman atas pengujian yang telah dilakukan atas Pengendalian umum perusahaan:

Secara keseluruhan, general control perusahaan dinilai sudah cukup memadai. Akan tetapi masih terdapat beberapa kelemahan pada general control yang diterapkan perusahaan, yaitu:



Gambar 2. Struktur Organisasi Opus 01

Tabel 1. Pemahaman Pengendalian umum FO O01.

No.	Komponen *General Control*	Ya	Tidak	Tingkat Pengendalian
1.	Administrasi Fungsi *Information Technology*	4	3	Cukup Memadai
2.	Pemisahan Tugas-Tugas IT	0	4	Tidak Memadai
3.	Pengembangan Sistem	4	2	Cukup Memadai
4.	Keamanan Fisik dan *Online*	10	4	Memadai
5.	*Backup* dan *Contingency Planning*	2	2	Cukup Memadai
6.	*Hardware Control*	1	2	Tidak Memadai
Total		21	17	

Sumber: Hasil Penelitian

1. Minimum persyaratan password masih bersifat sederhana dan user ID yang diberikan tidak bersifat unik.

2. Perusahaan belum memiliki dan menerapkan prosedur back up atas data yang penting, seperti data terkait inventory dan penjualan.

3. Perusahaan belum memiliki *disaster recovery planning*.

Password yang sederhana dapat meningkatkan risiko akses ke program dan data oleh pihak yang tidak diotorisasi. password hanya terdiri dari 4 karakter padahal password dinilai kuat jika terdiri dari 8 karakter, yang mana karakter password merupakan gabungan dari karakter angka dan huruf. User ID yang diberikan adalah nama

depan masing-masing karyawan. Ini akan meningkatkan risiko tersebarnya user ID ke pihak yang tidak diotorisasi, pengendalian utama terhadap penggunaan user ID dan password adalah menjaga kerahasiaan atas password.

Perusahaan telah memiliki compensating control atas kelemahan di atas, yaitu dibedakannya modul yang diaktifkan pada masing-masing komputer. Misalnya, pada *cash register* modul yang diaktifkan hanyalah modul POS. Direksi adalah orang yang memegang otorisasi dan mendapatkan *access priviledge* atas semua data dalam perusahaan. Direksi tidak bisa mengakses database langsung melalui komputer yang berada di cash register.

Semua data terkait penggunaan software Corsus disimpan terpusat pada database di server. Hal ini akan meningkatkan risiko kehilangan data karena server sebagai satu-satunya tempat penyimpanan data. Sebagai contoh, transaksi penjualan yang dimasukkan oleh Kasir langsung disimpan ke database server tanpa disimpan terlebih dahulu di komputer cash register. Begitu pula pemasukan data oleh divisi yang lain, seperti *Administrator*, *Warehouse*, dan *Finance Accounting*, langsung disimpan ke database server. Walaupun sampai sekarang hal ini belum terjadi.

Walaupun masih ada kelemahan, namun unsur control lainnya telah memenuhi pengendalian umum di perusahaan, sehingga pengendalian umum dapat disimpulkan cukup memadai.

Untuk melengkapi control pada aktivitas penjualan, perusahaan mempertahankan beberapa pengendalian manual yang dapat dipakai pada application control, yaitu:

1. Otorisasi transaksi penjualan melalui persetujuan dari customer.
2. Otorisasi pemberian diskon bagi member dan pembatalan penjualan oleh SOM (Sales Manager) atau SOM Assistant.
3. Kasir tidak memiliki wewenang untuk mengubah harga jual.
4. Kasir mencocokkan jumlah barang yang dibeli dengan jumlah record dalam tampilan Modul POS Corsus.

4.2. *Hasil Pengujian Pengendalian Aplikasi*

Tabel 2. Pemahaman Pengendalian Aplikasi Perusahaan.

No.	Komponen *Application Control*	Ya	Tidak	Tidak Relevan	Tingkat Pengendalian
1.	*Input Control*	13	1	3	Memadai
2.	*Process Control*	5	0	0	Memadai
3.	*Output Control*	5	0	0	Memadai
Total		23	1	3	

Sumber: Hasil Penelitian

Software Corsus digunakan dalam aktivitas penjualan dan pembelian serta pencetakan barcode pada *price tag* produk. Pengujian atas pengendalian aplikasi dibatasi pada siklus penjualan saja. Perusahaan menggunakan modul POS yang terdapat pada Corsus. Modul POS terdapat pada cash register dan digunakan oleh kasir.

Input control yang diterapkan oleh perusahaan telah memadai. Data yang diinput oleh kasir adalah *barcode* pada *price tag* produk. Tentunya *barcode* yang di-*scan* adalah produk yang akan dibeli oleh customer. Kasir harus mendapatkan persetujuan dari customer terlebih dahulu. Corsus menyediakan beberapa pengendalian untuk memastikan kebenaran data input, seperti *field check*, *sign check, limit* dan *range check, completeness check, validity check*, dan *reasonableness check.* Selain itu, Corsus secara otomatis memunculkan pesan error jika terjadi kesalahan input.

Pengendalian terkait batch input dinilai tidak relevan dengan proses input atas transaksi penjualan yang dilakukan. Terdapat satu kelemahan pada input control, yaitu *cancellation* dokumen yang dilakukan kasir hanya berdasarkan pemisahan tempat. Ini memungkinkan adanya kesalahan bahwa barcode produk yang sudah di-scan tercampur dengan barcode yang belum di-scan. Namun, kasir melakukan pemeriksaan kembali dengan membandingkan perhitungan jumlah barang secara fisik sebelum barang dimasukkan ke dalam kantong belanja dengan jumlah record atas *barcode* yang telah di-*scan*. Ini dapat menjadi *compensating* control atas kelemahan *cancellation* dokumen.

Process control dan *output control* yang dilakukan dinilai telah memadai. Sebelum pemrosesan data, Corsus melakukan pencocokan terlebih dahulu atas *barcode* yang dibaca oleh *barcode reader* dengan *barcode* yang terdapat dalam *database inventory*. Corsus akan menggunakan file yang benar dan pantas pada saat pemrosesan data. Database terkait barcode tersebut hanya berada dalam database di server. *Input control*, kasir diharuskan melakukan scan atas barcode barang yang dibeli oleh customer. Corsus juga menyediakan beberapa pengendalian untuk memastikan kebenaran data input. *Process control* yang dilakukan dinilai telah memadai. Laporan yang dihasilkan telah bernomor urut sehingga memudahkan proses pencarian ulang. Berdasarkan hasil penelitian di atas, pengendalian umum dan pengendalian aplikasi perusahaan sudah cukup memadai.

4.3. *Penentuan Ruang Lingkup Audit Siklus Penjualan dan Biaya Audit*

Adanya pengendalian umum dan aplikasi yang memadai, menghasilkan *Control risk* terkait penggunaan IT penjualan yang dinilai rendah. *Control risk* yang rendah artinya pengendalian intern terkait penggunaan IT dinilai mampu untuk mendeteksi atau mengoreksi salah saji. Pengendalian IT yang sudah memadai akan berpengaruh terhadap keputusan auditor mengenai penentuan ruang lingkup audit. Hubungan antara Komponen risiko audit dengan ruang lingkup audit dihubungkan pula dengan biaya audit, dijelaskan di bawah ini. Ruang lingkup audit dijabarkan melalui empat faktor utama, yaitu:

1. *Nature*. Pengendalian IT yang memadai dapat mengurangi *test of transaction* dan *test of balances*. Audit akan lebih efektif jika memperbanyak *test of control.*

Adanya pengurangan *test of transaction* dan *direct test of balances* akan mengurangi *working hours auditor*, sehingga dari unsur ini *fee audit* untuk auditor dapat dikurangi.

Akan tetapi, penomoran *sales transaction* yang dihasilkan secara otomatis oleh *software Corsus* dengan format yaitu "tanggal transaksi. urutan transaksi pada hari itu". Tanggal transaksi terdiri dari 6 digit karakter numeric dengan format DDMMYY. Sebagai contoh, tertulis receipt: 090713.013. Kode *sales transaction* 090713 sebagai tanggal transaksi yang berarti transaksi terjadi pada tanggal 9, bulan ke-7 bulan Juli, tahun 2013. Jika pada hari berikutnya terjadi transaksi penjualan yang pertama maka kode *sales transaction* pada *receipt* adalah 100713.001.

Asersi *completeness* adalah salah satu asersi yang diuji pada siklus penjualan. Pengujian asersi *completeness* biasanya dilakukan dengan pengujian sequence, dokumen telah berurutan dan tidak ada nomor yang hilang atau terlewat. Namun, sistem penomoran sales transaction tidak berlanjut dari hari ke hari sehingga diperlukan prosedur lebih lanjut. Hal ini menyebabkan perlunya penambahan *test of transaction* untuk menilai asersi *completeness*. *Test of transaction* dapat dilakukan dengan cara melakukan perbandingan antara jumlah transaksi per hari yang terdapat pada laporan penjualan harian dengan urutan transaksi terakhir pada hari tertentu.

2. *Timing*. Pengendalian IT dinilai telah memadai maka waktu pelaksanaan audit dapat dilakukan pada periode berjalan (interim). Artinya sampel yang diambil saat interim tidak sebanyak bila audit dilakukan pada akhir tahun, dengan kata lain biaya audit dari unsur inipun dapat dikurangi.

3. *Extent*. Pengendalian IT dinilai telah memadai maka jumlah bukti audit yang harus dikumpulkan auditor dapat dikurangi, sehingga dari sudut extent inipun biaya yang diperlukan dalam audit dapat dikurangi. Walaupun, untuk mendapatkan kepastian yang layak terkait asersi completeness pada transaksi penjualan, auditor harus mengumpulkan bukti audit yang lebih banyak.

4. *Staffing*. Pelaksanaan pengujian audit tidak memerlukan penggunaan spesialis. Personil yang melakukan pengumpulan bukti harus mempunyai kemampuan untuk memahami siklus bisnis perusahaan dan kemampuan terkait prosedur audit yang akan dilakukan. Karena staf yang melakukan audit bukan dari spesialis maka biaya audit yang diperlukanpun dapat dikurangi

5. Kesimpulan

Menjawab identifikasi masalah pertama, hasil evaluasi pengendalian umum dan pengendalian aplikasi atas siklus penjualan di FO 01, dapat disimpulkan bahwa Pengendalian umum dan aplikasi yang diterapkan telah memadai.

Perusahaan sudah menerapkan komponen dalam pengendalian umum, seperti administrasi fungsi IT, pengembangan sistem, keamanan fisik dan online, *back up* dan *contingency planning*, serta *hardware control*. Di sisi lain, masih terdapat kelemahan pada pengendalian umum, khususnya pada komponen pemisahan fungsi-fungsi IT. Namun telah ada compensating control untuk mengurangi risiko atas akses pihak yang tidak diotorisasi.

Corsus telah memiliki pengendalian yang memadai dalam semua komponen Pengendalian aplikasi. Dalam input control, kasir diharuskan untuk melakukan scan atas barcode barang yang dibeli oleh customer, Serta pengendalian untuk memastikan kebenaran data input. Pada Process control telah digunakan file yang benar dan pantas saat pemrosesan data. Database terkait barcode hanya berada dalam database di server. Corsus menyediakan fitur log yang merekam semua aktivitas kasir atas modul POS. Corsus akan memunculkan pesan error jika terjadi kegagalan pemrosesan transaksi. Output control pada Corsus melalui Laporan yang dihasilkan hanya bisa dicetak oleh kasir, dan diberikan kepada pihak yang telah diotorisasi. Laporan diberi nomor urut sehingga memudahkan proses pencarian ulang.

Menjawab identifikasi masalah ke dua, yaitu hasil uji Pengendalian umum dan aplikasi yang telah memadai, atas dasar tersebut, control risk terkait penggunaan IT siklus penjualan dinilai rendah. Control risk yang rendah berarti pengendalian intern yang sebagian besar terkait penggunaan IT dinilai mampu mendeteksi atau mengoreksi salah saji. Keputusan auditor atas ruang lingkup audit yang dikelompokkan dalam aspek nature, timing, extent, dan staffing dapat dipersempit

Akhirnya, Efisiensi biaya Audit dilakukan melalui, penggunaan IT dalam menangani operasional perusahaan telah menghasilkan laporan yang lebih berkualitas sehingga meminimalkan risiko laporan akan keliru. Dari sudut Nature tidak perlu melakukan substantive test dan test of ending balance; segi Timing - pelaksanaan audit interim mengurangi biaya sampel; segi Extent - jumlah bukti yang dikumpulkan dinilai sedang, sehingga tidak perlu biaya besar; Sedangkan untuk staffing, audit tidak memerlukan penggunaan spesialis yang berarti biayapun dapat dikurangi. Hasil penelitian menunjukkan bahwa efisiensi biaya dapat dicapai, dan semakin kuatnya pengendalian umum dan aplikasi dalam perusahaan dapat mengurangi biaya audit lebih efisien lagi.

Daftar Rujukan

Arens, Alvin A., Randal J. Elder dan Marks S. Beasley. 2012. *Auditing and Assurance Services: An Integrated Approach*. England: Pearson Education Limited.

Bodnar, George H., dan William S. Hopwood. 2001. *Accounting Information System*. Eight Edition. New Jersey: Prentice-Hall, Inc.

Boynton, William C. dan Raymond N. Johnson. 2006. *Modern Auditing Assurance Services and The Integrity of Financial Reporting*. United States of America: John Wiley & Sons, Inc.

Dube, D. P., V. P. Gulati. 2005. *Information System Audit and Assurance*. New Delhi: Tata McGraw-Hill.

Hall, James A. dan Tommie Singleton. 2005. *Information Technology Auditing and Assurance.* Ohio: Thomson South-Western.

IAASB (International Auditing and Assurance Standards Board). 2012. *Handbook of International Quality Control, Auditing Review, Other Assurance, and Related Services Pronouncement.* New York: IFAC.

IAPI (Institut Akuntan Publik Indonesia). 2011. *Standar Profesional Akuntan Publik*. Jakarta Selatan: Salemba Empat.

Moeller, Robert R. 2007. *COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework.* USA: John Wiley & Sons, Inc.

Rittenberg, Larry E. dan Bradley J. Schweiger. 2005. *Auditing, Concepts for a Changing Environment, edisi 5.* Ohio: Thomson South-Western.

Romney, Marshall B. dan Paul John Stienbart. 2009. *Accounting Information System, edisi 11.* New Jersey: Pearson Education Limited.

Sekaran, Uma dan Roger Bougie. 2010. *Research Methods For Business: A Skill Building Approach.* United Kingdom: John Wiley & Sons, Inc.

Weber, Ron. 1999. *Information Systems Control and Audit.* New Jersey: Prentice-Hall, Inc.